THE CIP REPORT

CENTER FOR INFRASTRUCTURE PROTECTION VOLUME 10 NUMBER 3
AND HOMELAND SECURITY

SEPTEMBER 2011
9/11: 10TH ANNIVERSARY

Click here to subscribe. Visit us online for this and other issues at http://cip.gmu.edu

This month, as we all reflect on the ten years since 9/11, we look at lessons learned regarding critical infrastructure protection (CIP) as a result of the tragic events of September 11, 2001.

GEORGE MASON UNIVERSITY
School of Law
CENTER for INFRASTRUCTURE PROTECTION and HOMELAND SECURITY

We begin with the changes in the field of critical infrastructure protection since 9/11 and then examine the uncertainties we are faced with as a result. We present articles on the progress and evolution of CIP over the last ten years, lessons learned at the Department of Homeland Security, adaptability of CIP and the 9/11 attacks in New York, and emergent and strategic behavior during restoration. An article on the Transportation Sector discusses the evolving focus on security and we present an interview with a Virginia State Trooper on lessons learned in law enforcement. We take a look at cybersecurity, 9/11 memorials, and a brief overview of the recent hearing on preventing terrorist travel.

Given that September is also National Preparedness Month, we include information about Presidential Directive 8.

This month's *Legal Insights* examines the challenges involved with overlapping jurisdictions and regulations in critical infrastructure protection.

We would like to take this opportunity to thank the contributors of this month's issue. We truly appreciate your valuable insight.

We hope you enjoy this issue of *The CIP Report* and find it useful and informative. Thank you for your support and feedback.

Mick Kicklighter
Director, CIP/HS
George Mason University, School of Law

Some Changes in the Critical Infrastructure Field since 9/11

by Dr. Robert Miller,*
Professor, National Defense University

On September 11, 2001, I was at Hurlburt Field in Fort Walton Beach. Along with colleagues from the Federal Bureau of Investigation (FBI) and what was then known as the Joint Task Force on Computer Network Defense (JTF-CNO), we were there to talk to students at the U.S. Air Force Special Operations School about threats to critical infrastructure, particularly information infrastructure. Understandably, the students turned out to be more than a bit distracted. Well, so were we.

On the long drive back to Washington the next day (planes were, of course, grounded), my colleagues and I talked about how things were likely to change. We of course knew about Al Qaeda and were pretty sure that Osama bin Laden and his henchmen were responsible for the attacks. As we drove past the still-smoking Pentagon on our way to pick up our cars at National Airport, we agreed that many things, including critical infrastructure policy, were about to change quickly and drastically.

And so they have.

The world is a different place than it was a decade ago, and there have been many alterations to ensure its protection, including in the field of critical infrastructure. However, four major changes stand out. Three of these are fairly well along, and the fourth is still developing.

The most obvious change stems from the creation of the U.S. Department of Homeland Security (DHS) and the development of a durable institutional framework for government policy in the critical infrastructure field. In 2001, there was still confusion about who was in charge of what. The Critical Infrastructure Assurance Office (CIAO) had a wide-ranging mandate but little money and no real power. The demarcation lines between the CIAO, FBI, Department of Defense (DoD), and other entities were (to be charitable) a bit fuzzy. All of this is far from settled today, but roles and responsibilities are much clearer than they were then. A variety of laws and directives have helped clarify issues. Notable among these are the 2002 Homeland Security Act (P.L. 107-296) and Homeland Security Presidential Directive (HSPD) 7 (2003). DHS has responded to its new responsibilities by issuing several versions of the National Infrastructure Protection Plan (NIPP) (2006, 2009) as part of an overall set of policy documents that also includes the National Incident Management System (NIMS) and the National Response Framework with its supporting annexes, including one on critical infrastructure. Since Hurricane Katrina, DHS has made some significant strides in developing an overall structure that coordinates critical infrastructure planning, risk management, emergency management, and cybersecurity, among others. DHS has also attempted to categorize critical infrastructure and assets and systems according to criticality. This is still a work in progress, but a substantial start on this complex effort has been made. Furthermore, analysis and information-sharing have both been improved significantly, through such means as protective security advisors, State and local fusion centers, and the National Cybersecurity and Communications Integration Center. Although progress in these areas has often seemed slow to those on the ground, some undeniable improvements have taken place. DHS recently released a "progress report" on the government's improvements since 9/11 (DHS, *Implementing 9/11 Commission Recommendations, A Progress Report*, July 2011); they do have a great deal to talk about — and, as they would acknowledge, a great deal more to do. The new Presidential Policy Directive (PPD) 8 ("National Preparedness," March, 2011) may help in this area.

A second change has to do with

(Continued on Page 34)

Coming to Grips with Uncertainty

by Samuel H. Clovis, Jr., Doctor of Public Administration
Professor and Chair, Department of Business Administration and Economics,
Morningside College, Sioux City, IA

In my day job, I am a tenured professor at a small liberal arts college in the Midwest. As our main focus is teaching undergraduates, we must deal with all the issues associated with modernizing our pedagogies to accommodate social media, rapid advances in technology, and generational divides that often leave my colleagues and I perplexed. We soldier on, doing our best to keep up with the younger, hipper members of our teaching cadre. Though we try to bring civic responsibility into our curricula, making sure that students do their homework and show up for class are often at the top of the priority list. Do not get me wrong, it is a blessing to be at such a good school with really good students. However, I can say without qualification, that I do not remember discussing protection of critical infrastructure in any of my classes. Perhaps this is my failing, but the topic just does not seem to come up. Though the events of 9/11 occurred in these students' lifetimes, they do not include it in their daily calculus. Such is not the case with graduate students.

During the past three years, my affiliation has been with the Center for Homeland Defense and Security at the Naval Postgraduate School in Monterey, CA. These students, earning masters degrees through the auspices of DHS, are some of the top homeland security professionals in the country. As the Nation continues to languish in a slow economic recovery that has put tremendous pressure on State and local governments, many of these wonderful civil servants are concerned about the confidence citizens might have in government at the national, State, and local levels. This lack of confidence, verified in national polls, creates tensions between government officials and citizens and between officials at different levels of government. This tension and lack of confidence similarly feeds a sense of uncertainty that has deleterious effects on the private sector. The uncertainty manifests itself in defensive pathologies that inhibit cooperation and collaboration. Without cooperation between levels of government and between the private and public sector, enhanced infrastructure protection becomes problematic. Raising confidence in government will take better performance at all levels. Focusing on efforts to continue to increase resilience and continuity of business operations is still possible in spite of current conditions.

One of the textbooks used in my strategic management course introduces an excellent template for enhancing strategic thinking. The basic premise is that reducing uncertainty is one of the most important tasks assigned to strategic leaders. To begin the process of reducing uncertainty, one must have an appreciation for the remote influences found in the external environment that might affect business operations at some point in the future. Those remote influences, over which one might have little control, are found in the areas of politics, social change, economics, technology, and ecology. Correctly identifying trends in these areas will help decision-makers begin the process of mitigating uncertainty. Does government affect these influences in any way? Of course it does, and a lack of confidence in government affects all other business operations.

We live in a politically divided country where the gulf continues to widen between left and right with each subsequent Congress. Business enterprises and the business community writ large are affected by the political infighting that has become the norm in American politics today. Institutional pathologies found in Congress and the executive branch have done little to encourage confidence in government, and the perception that government seems interested in developing competition-killing regulatory regimes, maintaining

(Continued on Page 27)

Progress and Evolution of Critical Infrastructure Protection over the Last Ten Years?

by Fred Cohen, Fred Cohen & Associates

The question was posed as to whether and to what extent critical infrastructure protection has changed in the last ten years. In my opinion, this includes the question of whether such changes have improved the situation. Let us start with the underlying nature of the question.

It seems that while many changes can be readily identified, there is no basis today for determining whether or to what extent any such changes have made protection more or less effective. Indeed, the most fundamental change needed to address this issue is the movement toward a science of protection, which has not been seriously undertaken, at least in some areas. As a result of the lack of scientific study and a widely accepted scientific basis, there is no meaningful way to make sensible measurements of protection, and thus the notion of improvement cannot be realistically assessed. But perhaps more detail would be helpful in bringing clarity to this issue.

What Changes have been Made?

As a starting point, it should be noted that there have been many changes in protection associated with critical infrastructures of late. Starting in the late 1990s, when the President's Commission on Critical Infrastructure Protection (PCCIP) identified the need at a national basis to make changes in the United States, a vision of a future state was notionally present. But, at the time, that vision was not being realized at a rapid rate. Then the September 11, 2001 attacks on U.S. soil took place, leading ultimately to a dramatic change in the posture of the United States and much of the rest of the world with regard to protection.

Unfortunately, to many knowledgeable and skeptical observers, many of these changes were of little technical value other than from a perception perspective. Issues such as increased levels of invasiveness and inconvenience in airport searches were not met by published or identified measurements of effectiveness. Testing repeatedly showed that the countermeasures in place could be readily bypassed. A system of continuous "improvement" based on reducing the potential for the "last attack" were applied with little apparent effect other than to make travel less convenient, more costly, and more invasive to the traveling public with perhaps a marginal but unmeasured benefit in reducing copy-cat attacks. The feeling of safety and level of suspicion engendered by such measures has the — again unmeasured — likely effect of making individual and poorly trained threat actors more nervous and more likely to be detected and interdicted while making the public at large feel safer, with the benefits of these results quantitatively unknown and somewhat speculative.

Other less obvious changes were perhaps somewhat more technically effective, although again, measurement has not been widely published if it has been undertaken in a meaningful way at all. For example, water systems, pipelines, power systems, telecommunications, and other similar systems have been examined at some level of depth to better understand the potentials for harm and the limitations of existing protective mechanisms. While the increased scrutiny is, presumably, a benefit in terms of general and situational awareness, and the increased focus of attention and resources on these issues has the potential to increase knowledge, evidence of the utility of these presumed benefits is lacking and no system of measurement has been widely identified and applied to provide meaningful metrics.

Lacking a system of measurement and a standard against which to measure, it is doubtful we can determine, based on fact, whether protection is better or worse today than it was ten years ago.

(Continued on Page 5)

Evolution *(Cont. from 4)*

Some Things We May be able to Measure in Some Areas

By focusing on select areas of protection, additional insight may be gained. The particular areas chosen here include the information protection arena with focus on general purpose computing at enterprises, by individuals, and in government, which is vital to several critical infrastructure sectors (e.g., finance, government, telecommunications, logistics), and on industrial control systems, which are vital to more traditional critical infrastructure sectors (e.g., power, water, fuel, manufactured goods, and transportation). Within these areas, there are various issues that are commonly considered, some of which are identified here and discussed in terms of changes over the last ten years. This represents only my qualitative assessment and is without adequate basis in measurement to be treated as definitive in any meaningful way. As discussed, measurement in these areas is currently problematic.

Risk Issues:

Threats: It appears that more and more skilled, organized, and resourced threat actors have been identified and are active in 2011 than in 2001. However, to my knowledge, there is no systematic reporting of or method for identifying and characterizing such individuals and groups available in any public forum. While there are groups that produce reports and provide databases on these issues, none of them appear to be adequately supported by base rates or detailed methodologies to support sound conclusions about situations at any given time or as it changes with time.

Vulnerabilities: It appears, based on publicly available databases like the Open Source Vulnerability Database (OSVDB) and national vulnerabilities databases such as the MITRE database on vulnerabilities, that the rate of widely published vulnerabilities has increased. However, this tends to ignore many of the widely known vulnerabilities that are not directly technical in nature, such as exploitations of people, systems, architectures, and similar issues. For example, malicious programs that are downloaded and run by users represent vulnerabilities that are ignored by such collections and often dominate the events of interest. Interconnection and architectural vulnerabilities have increased for ICS systems so that it is clear that there are more paths to attach such systems. Many such systems do not have the same sort of mechanisms or protections feasible today as more general purpose Internet connected computers. This can reasonably be seen as an increase in vulnerability if measured in terms of the size and number of links from external sources to targets in the attack graph. But as a metric, it is unclear whether this is useful for understanding the overall situation. For example, insiders remain responsible for much of the reported damage attributed to sources, and thus external connectivity changes may be of relatively limited impact in terms of overall security.

Consequences: The consequences of attacks are rarely available for review as they tend to be closely guarded secrets. While the widely publicized consequences are seemingly bigger and more frequent today than ten years ago, as seen by the DataLoss.Org website and other published reports, reporting requirements have increased as has publication of events, while speculation about consequences has been lacking in the published reports. When consequences are available, the lack of a common method of valuation for information-related losses or content leads to a set of numbers that are not comparable and thus fail to support any meaningful conclusions against a standard or over time.

Interdependencies and Risk Aggregation: The analysis necessary to support definitive answers in this regard is, again, not available. But it seems almost certain that analysis would show that aggregation of risks and interdependencies have dramatically increased over the last ten years. There is little available data to support substantial conclusions from losses in this regard; however, the effects of risk aggregation and common mode failures have produced dramatic results, including the nuclear reactor problems in Japan, the WikiLeaks classified leak incident, and any number of large-scale events involving information technology (IT). What is unclear is whether the situation is in fact getting any worse since, in

(Continued on Page 6)

Evolution *(Cont. from 5)*

addition to the lack of measurement, mandatory reporting has increased only for leaks of privacy-related information and select critical infrastructure incidents. Even for reported cases, valuation methods are not available and quantification is not based on a standard. The rationale for asserting that the problem has worsened is the increased complexity and integration of systems into larger information mechanisms. For example, identity management has substantially moved ahead. Along with it, federation of identities and the use of centralized servers for control of these processes obviously places increased risk on the small number of servers leveraged to larger effect and adds interdependencies that were not previously present. However, the economies of scale and quality of such systems may compensate for the aggregations by providing higher surety for more systems. Again, without a system of measurement, no basis for meaningful metrics can be supported.

Risk Management Approaches: The four basic approaches (transfer, acceptance, avoidance, and mitigation), have not changed over the last ten years, and this field appears to be relatively static. It appears that the tolerance for risk has increased in the information arena, but this may be the result of a lack of understanding of the issues rather than a conscious or knowing decision by decision-makers.

Protection Objectives:

• Integrity protection capabilities have improved to some extent in large numbers of computers as the Trusted Computing Group's trusted platform module integrity mechanisms have been increasingly deployed over the last decade; however, these mechanisms go largely unused for anything other than limited digital rights management. Meanwhile, systems like mobile devices, which are increasingly dominating the consumer market and pushing into enterprise markets, largely lack longstanding integrity mechanisms such as hardware process separation and file systems security. Again, we have no sound method for measuring any actual change in integrity protection.

• Availability of hardware has improved with technological advancements, and software checking has improved availability along with operating system improvements for widely deployed operating environments like Windows. At the same time, server software has become more complex and interdependent, and no widely available measurements of availability have been identified that could address the overall question of availability. Furthermore, the movement to mobile devices has dramatically changed the nature of availability since access and utility has increased from a wide range of locations where access was previously very expensive and not widely available. Again, depending on what is chosen to measure, different results will appear. It is, however, obvious to most observers that accessibility to services has made a dramatic shift in the positive direction with the increased availability of WiFi and cellular services supporting smart-phones, pad computers, and netbook platforms.

• Confidentiality has been problematic in the rapid growth of Internet technologies and the push toward gaining efficiencies of scale. Many major disclosures of leaks have driven the perception of a worsening situation, but again, no metrics are really available that are comprehensive in nature. Large-scale leakage of classified information to the media associated with the WikiLeaks case appears to be unprecedented, but it is unclear how this affects critical infrastructures.

• Use control is apparently being loosened as mobility increases and information work is increasingly outsourced and physically distributed. More and longer chains of interdependencies appear to be present today than ten years ago. This leads to use control problems, increasingly seen in published attacks, that gain access to user interfaces which are then exploited to attack systems with which the users have access. But again, metrics in this area are lacking and the lack of detection does not translate into a lack of actual attack. More detections may mean fewer attacks persist.

• Accountability is increasing in many systems and

(Continued on Page 28)

Incorporating Lessons Learned at the Department of Homeland Security

by Todd M. Keil, Assistant Secretary for Infrastructure Protection,
National Protection and Programs Directorate

Protecting the Nation's critical infrastructure has been a key mission of DHS since its establishment. When the Hart-Rudman Commission originally discussed the idea for a "homeland security agency," it called for a "Directorate for Critical Infrastructure Protection" that would oversee the physical assets and information networks that make up U.S. critical infrastructure. The "agency" would coordinate efforts to address risks to cyber and physical critical infrastructure assets. In response to these recommendations, the Office of Infrastructure Protection was formed and is now an element of the Department's National Protection and Programs Directorate (NPPD).

In 2006, DHS introduced the NIPP to provide the unifying structure for the integration of public and private sector programs and activities. The NIPP was updated in 2009 to integrate the concept of resilience and to expand programmatic focus to account for natural as well as manmade hazards. Since its inception, the Department has learned many lessons about how to strengthen the protection and resilience of critical infrastructure assets, systems, functions, and networks. This article highlights several of those key lessons.

Most Critical Infrastructure is Privately Owned; Therefore, Voluntary Public-Private Partnerships are the Cornerstone of Critical Infrastructure Protection

DHS and its Federal, State, and local partners have built a security architecture that allows us to better identify, mitigate, and respond to the threats that the Nation faces. Under the NIPP framework, DHS meets regularly with governmental entities, critical infrastructure sector councils, and other private sector partners to share information and to develop and distribute tools. For example, the Voluntary Chemical Assessment Tool enables the evaluation of risk and encourages implementation of protective actions. DHS has also collaborated with private sector partners to develop numerous Webinars and online courses based on stakeholder needs, such as "Workplace Security Awareness" and "Active Shooter: What You Can Do."[1]

Assistant Secretary Keil at the World Trade Center construction site, in front of the Museum Pavilion, New York City, April 2011. *Photo courtesy of DHS.*

An All-Hazards Approach to Risk Management is Vital to Increasing Preparedness

When people think about risks to critical infrastructure, they usually attribute those risks to acts of terrorism.

(Continued on Page 8)

1. For information about VCAT, see http://www.dhs.gov/files/programs/gc_1260467577301.shtm. To learn about infrastructure-related training programs, see http://www.dhs.gov/files/training/training-critical-infrastructure-partners.shtm.

DHS *(Cont. from 7)*

However, risks to critical infrastructure can also be caused by natural hazards, industrial accidents, and insider and lone wolf attackers. The Department recognizes that the threats facing our country are continuously evolving, which means that our efforts must also continue to evolve.

Many critical infrastructure owners and operators, government emergency managers, and first responders have developed strategies, plans, policies, and procedures to prepare for, respond to, and recover from a variety of natural disasters and other threats. DHS supports these efforts through national information-sharing networks, risk management frameworks, and public-private coordination structures that support preparedness for all types of hazards. The Department provides real-time information sharing and coordination of response and recovery efforts during emergency incidents through the National Infrastructure Coordinating Center and the 93 Protective Security Advisors (PSAs) deployed across all 50 States.

Disasters and Incidents Often Cause Ripple Effects across a Region's Infrastructure Systems and the Services they Support

The direct impact, disruption, and cascading effects of natural disasters and other threats are well documented and underscore the vulnerabilities and interdependencies of the Nation's critical infrastructure. Major disruptions to one or more elements of the critical infrastructure network could lead to devastating losses to communities, regions, and the Nation as a whole. Numerous disasters have affected critical infrastructure systems and have highlighted a need to better coordinate information sharing as well as response and recovery activities across jurisdictional boundaries. For example, in April 2011, Alabama experienced historic tornadoes. In the immediate aftermath, PSAs identified the impacts to critical infrastructure and operational capabilities. Employing the Department's online information sharing tools, these PSAs were able to quickly communicate with key stakeholders from government and industry to speed recovery efforts. The Department's role in the process proved valuable in understanding local and regional interdependencies and ensuring a coordinated response.[2]

Resilience Must be Part of the Critical Infrastructure Protection Equation

It is essential that the government and the private sector coordinate infrastructure protection and resilience programs and activities. DHS has developed the Regional Resiliency Assessment Program (RRAP) to help the public and private sectors understand the interdependencies involved in the operation of a critical assets, systems, functions, and networks. Through the RRAP, DHS utilizes assessment and survey methodologies to examine critical infrastructure vulnerabilities, threats, and potential consequences from a regional, all-hazards perspective. These methodologies enable DHS to identify dependencies, interdependencies, cascading effects, and capability gaps, while synthesizing resilience measures to be shared with the wider critical infrastructure stakeholder community.

Critical Infrastructures Rely on the Efficient Operation of Information Systems and Networks that are Vulnerable to Cyber Threats

The Nation's critical infrastructure faces a variety of cyber risks, including intentional attacks by malicious actors, insider threats, technological failures, human error, and supply chain vulnerabilities.[3] DHS cybersecurity tools and resources help private sector network owners and operators address a range of cyber issues ranging from the identification of threats and vulnerabilities to the development of risk management strategies within and across critical infrastructure sectors. For example, DHS cyber experts can perform assessments of cyber networks and provide guidance on how to better secure them. The Department leverages trusted relationships with private sector companies and Federal departments and agencies to provide technical expertise,

(Continued on Page 9)

2. Learn more about Protective Security Advisors at http://www.dhs.gov/files/programs/gc_1265310793722.shtm.
3. See July 2011 *The CIP Report* on managing and protecting the global supply chain.

DHS *(Cont. from 8)*

including onsite analysis, mitigation support, and assessment assistance. DHS also works to mitigate threats to cyber networks to reduce future risks. In October 2009, DHS opened the new National Cybersecurity and Communications Integration Center (NCCIC) — a 24-hour, DHS-led coordinated watch and warning center to serve as the Nation's principal hub for organizing cyber response efforts and maintaining the national cyber and communications common operational picture. DHS also implemented the Cybersecurity Partners Local Access Plan, which allows security-cleared owners and operators of critical infrastructure, as well as State technology officials and law enforcement officials, to access secret-level cybersecurity information via local fusion centers. In July 2010, a real-world threat emerged that significantly changed the landscape of targeted cyber attacks on industrial control systems. DHS analysts concluded that this highly complex computer worm was the first of its kind and was written to specifically target mission-critical control. The Department shared information about the new threat and coordinated mitigation actions with critical infrastructure asset owners and operators from the public and private sectors.

The Department works closely with government and industry organizations, providing advisories and updates to the industrial control systems community for detecting an infection and mitigating threats. Going forward, DHS will continue to work with the cybersecurity community to investigate other threats and vulnerabilities through analysis, assessments, onsite incident response activities, information sharing, and partnerships.

Effective Information Sharing Requires an Understanding of the Information Needs of Critical Infrastructure Partners

To promote effective decision-making, the Federal government needs to provide the right information to the *right* people at the *right* time. Through the Critical Infrastructure and Key Resources Information Sharing Environment (CIKR ISE), DHS works to develop an understanding of stakeholders' information-sharing needs in order to provide access to actionable information.[4] One way that the CIKR ISE supports communication and information sharing among critical infrastructure owners and operators is through the DHS Suspicious Activity Report (SAR) process. Initiated to support the Nationwide SAR Initiative, DHS uses coordinated information sharing to channel reports of suspicious activity to appropriate authorities across the country and to relevant private sector stakeholders.

A Regulatory Framework is Necessary to Address Risks to Some Critical Infrastructure, and to Address Certain other Risks Faced by the Population at Large

The Nation's critical infrastructure continues to face persistent and evolving threats from both individuals and organized groups. Since 9/11, critical infrastructure owners and operators across 18 sectors[5] have initiated voluntary security programs and invested in security improvement projects to help address these threats. Still, securing high-risk facilities in the Chemical Sector, for example, requires more than voluntary efforts on the part of government and the private sector. DHS has leveraged knowledge and insight gained from experts, members of industry, academic, and Federal partners to develop and implement a regulatory framework that addresses the high level of risk posed by certain chemical facilities. In 2007, DHS adopted rules requiring high-risk chemical facilities to complete Security Vulnerability Assessments, develop Site Security Plans, and implement protective measures necessary to meet risk-based performance standards established by the Department.[6]

DHS is also engaged in other regulatory efforts to protect the public from use of dangerous chemicals in acts of terror. For

(Continued on Page 29)

4. Learn more about the CIKR ISE at http://www.dhs.gov/files/programs/gc_1292350623062.shtm.
5. The 18 critical infrastructure sectors are described at http://www.dhs.gov/files/programs/gc_1189168948944.shtm.
6. For more about the Chemical Facility Anti-Terrorism Standards (CFATS) program, see http://www.dhs.gov/files/programs/gc_1169501486179.shtm.

Adaptability of Critical Infrastructure and the September 11, 2001 Attacks in New York City

by Rae Zimmerman*

The infrastructure that provides electric power, transportation and goods, clean water and waste management services, and communication is critical to the social and economic environment to which we have become accustomed. It is also critical in emergencies as well as in "normal" times to evacuate people expeditiously and move supplies and services into affected areas to avoid magnifying injury and death. Dense urban areas are particularly challenging in their ability to recover from disasters, and the density can be used as an advantage. New York City's infrastructure is among the largest, and according the U.S. Census Bureau, some of the City's counties are in the top group of counties with the densest populations in the United States. New York City exceeds other cities by far, for example, in terms of passengers traveling on mass transit, the traffic volume on its roadways, and consumption of the basic services of electric power and water. The future viability of critical infrastructure faces numerous threats, as terrorist attacks internationally have shown. The City's systems are vulnerable due to the degree of concentration, their size and extensive networks, openness, and the ability to attract large numbers of people.

According to a 2011 Pew Center public survey, terrorism continues to be a top public priority in the United States since the September 11, 2001 attacks, ranking third among the priorities surveyed as it has for a few years.[1] In the weeks and months following the World Trade Center (WTC) attacks, New York City's infrastructure was challenged beyond what could have ever been imagined. The stories are numerous and the lessons are critical and need to be told over and over to guide the future.

In the hours, days, and weeks following the attacks, the city's public services were adapted in ways that were often not planned or anticipated. Debris was everywhere, creating obstructions in the streets that made evacuation difficult and hindered the ability of emergency vehicles to provide needed services to enter the area. Zimmerman and Sherman (2011) found that debris was identified by about two-thirds of survivors surveyed as an obstacle encountered when trying to leave the area.[2] The removal of debris, estimated at about 1.56 million tons, became a high priority before any other services could be restored in the long-term, and involved some of the largest construction firms, depended on the flexibility of city regulations for waste removal, and ultimately was completed by May 2002.[3]

Electric power and communications infrastructure could rebound relatively quickly through the deployment and acquisition of generators and cell towers through preexisting supply networks established for large events.[4] Electricity distribution followed a similar history. Shortly after the attacks, when two substations were destroyed, over 30 miles of distribution lines were routed over the existing street system to connect the disrupted area to substations outside the area. The immediate need for water to try and combat fires was provided by fire boats, though the fire fighting

(Continued on Page 11)

1. Pew Research Center for the People and the Press, *Less Optimism about America's Long-Term Prospects*, (January 20, 2011), 1, available at: http://people-press.org/files/legacy-pdf/696.pdf.
2. R. Zimmerman and M. Sherman, "To Leave An Area After Disaster: How Evacuees from the WTC Buildings Left the WTC Area Following the Attacks," *Risk Analysis*, 31 (5), (2011), 796.
3. R. Zimmerman, "Public Infrastructure Service Flexibility for Response and Recovery in the September 11th, 2001 Attacks at the World Trade Center," in *Beyond September 11th*, Natural Hazards Research & Applications Information Center, Public Entity Risk Institute, and Institute for Civil Infrastructure Systems, Boulder, CO: University of Colorado, (2003), 258, http://www.colorado.edu/hazards/publications/sp/sp39/sept11book_ch9_zimmerman.pdf.
4. Ibid, page 251.

Adaptability *(Cont. from 10)*

challenges ultimately were too great for that approach.

The recovery of transit exemplifies much of the flexibility needed to face critical infrastructure emergencies. The physical attributes of the City's transit system had an inherent flexibility and redundancy that was brought into play after an initial shutdown. Jenkins and Winslow[5] attribute this to the Metropolitan Transportation Authority's (MTA) long history of emergency planning from building collapses, the use of buses in evacuations as emergency shelters, and general exercises and training, all experiences that were brought to bear upon the WTC situation. Though massive communication problems occurred within the Tower itself, communications within the rail systems averted what could have been a worse catastrophe. Train operators invoked emergency procedures within a minute of the first plane hitting the North Tower by communicating with the MTA control center and Port Authority Trans-Hudson (PATH) emergency procedures began within six.[6]

The immediate extent of the damage and the recovery is important to recount along with the more extended history. On September 11, 2001, in the immediate vicinity of the attacks, some subway corridors were destroyed, such as the 1,400 feet of tunnel; others were flooded, including the 7th Avenue tunnel; stations were destroyed, such as the Cortland Street station and the PATH World Trade Center station; and others were obstructed, not to mention breakdowns in a lot of the equipment.[7] Yet, after the initial shutdown of all transportation systems, transit rebounded within hours, to a limited extent, and eventually rebounded to full service. Subway service resumed within NYC by having trains take advantage of their ability to bypass the WTC area using existing routes. The PATH system stations north of the WTC absorbed traffic from the WTC station that had been destroyed. The rail and bus transit systems showed initial signs of recovery within days to about two weeks.[8] On the day of the attacks, the ferry service also provided transport out of the city. Emergency services were provided by both formal and informal networks of organizations throughout the city and the region.

What keeps infrastructure viable in emergencies is its flexibility and in particular, the ability of evacuees and emergency services to take multiple routes between the same origin and destination and to attract the resources necessary to recover.[9] Innovation is a key to flexibility and robustness and has several dimensions. Innovation in the physical attributes that shape infrastructure is one dimension. Innovation in the way infrastructure is managed, operated, and maintained is another. This is a challenge given the shortfalls in estimated investment needs by the American Society of Civil Engineers (2011),[10] Zimmerman (2009),[11] and others. Disasters often prompt the immediate shutdown of infrastructure, which creates even more serious problems if alternatives are not designed into such strategies. A third dimension is the adaptability of human behavior in the face of disasters given the increasing dispersion and growth of population centers, especially close to hazard areas. The U.S. Census has recorded the continued growth of populations in coastlines that tend to have fewer

(Continued on Page 30)

5. B. M. Jenkins and F.E. Winslow, *Saving City Lifelines: Lessons Learned in the 9/11 Terrorist Attacks,* The Mineta Transportation Institute (MTI), San José State University College of Business, San José, CA, (2003), 29, http://www.transweb.sjsu.edu/mtiportal/research/publications/documents/02-06.pdf.
6. U.S. Department of Transportation (U.S. DOT), ITS Joint Program Office (ITS JPO), John A. Volpe National Transportation Systems Center, *Effects of Catastrophic Events on Transportation System Management and Operation: Cross Cutting Study*, Washington DC, Volpe Center, (2003).
7. Jenkins and Winslow, op cit., (2003), 27-28.
8. R. Zimmerman and J.S. Simonoff ,"Transportation Density and Opportunities for Expediting Recovery to Promote Security," *Journal of Applied Security Research*, 4, (2009), 48-59.
9. Zimmerman, op cit., (2003), 260.
10. American Society of Civil Engineers (ASCE), "Failure to Act," Reston, VA, USA: ASCE, (2011)
11. R. Zimmerman, "Making Infrastructure Competitive in a Changing World Through Investment," *The ANNALS of the American Academy of Political and Social Science*, 626 (1), edited by S. Wachter and E. L. Birch. Philadelphia, PA: AAPSS, (November 2009), 226-241.

Emergent and Strategic Behavior during Critical Infrastructure Restoration after 9/11

by David Mendonça, Associate Professor, Industrial and Systems Engineering Department, Rensselaer Polytechnic Institute; William A. Wallace, Professor, Industrial and Systems Engineering Department, Rensselaer Polytechnic Institute; and
Louis Calabrese, Assistant Vice President, Neuberger Berman, New York, NY

Using observations from the response to the September 11, 2001 attacks, this article addresses two common misconceptions concerning post-disaster repair of critical infrastructure systems. First, it is commonly assumed that infrastructure repair is best considered as a restoration task — that is, once immediate life- and property-saving activities have been completed. There is ample evidence to suggest that, due to a variety of factors, disaster response activities now depend crucially on services provided by critical infrastructures. Second, infrastructure repair is assumed to imply reconstruction of the pre-disaster system. Yet a close examination of post-disaster infrastructure repair shows that disasters continue to be sources of system renewal. Indeed, post-disaster infrastructure systems rarely, if ever, mirror pre-event systems. To address both misconceptions, research is needed to develop tools and techniques to enable services provided by infrastructure systems to be delivered to support response efforts, even as work is undertaken to design the new systems that will eventually be built.

Our studies of post-9/11 infrastructure restoration involve archival research, field observation, and interviews, essentially employing data from both human and machine sources.[1] This work is intended to complement more analytically minded research, usually directed towards identifying opportunities for optimizing restoration. Indeed, a main concern of this work is in identifying the extent of emergent, even improvised, behavior during restoration activities. An outgrowth of this research has been a number of prototype tools and technologies to support infrastructure restoration.[2,3] Given the acknowledged increasing connections among infrastructure systems, a particular focus of our work has been in identifying and modeling interdependencies among infrastructure systems, particularly those that have been subjected to sudden, catastrophic shock.

A close examination of infrastructure interdependence in New York City in the 13 weeks following the 9/11 attack illustrates the salience of infrastructure repair not only to recovery but to response.[4] Of the post-attack disruptions to critical infrastructures reported in the *New York Times*, approximately 35 percent involved some kind of interdependence. The majority of disruptions to banking, government, transportation, and emergency services infrastructures did not involve interdependency, while the reverse is true for power, telecommunications, oil and gas, and water. This latter group may therefore be regarded as more connected to other infrastructure systems than the former group. A more detailed analysis shows that correlations between a majority of all possible combinations of infrastructure pairs (e.g., power and

(Continued on Page 13)

1. David Mendonça and W. A. Wallace, "Impacts of the 2001 World Trade Center Attack on New York City Critical Infrastructures," *Journal of Infrastructure Systems*, 12(4), (2006), 260-270.
2. M. Chakrabarty and D. Mendonça, "Integrating Visual and Mathematical Models for the Management of Interdependent Critical Infrastructures," *IEEE International Conference on Systems, Man and Cybernetics,* The Hague, The Netherlands, October 10–13, (2003).
3. W.A.Wallace, D. Mendonça, E. Lee, J. Mitchell, and J. Chow, "Managing Disruptions to Critical Interdependent Infrastructures in the Context of the 2001 World Trade Center Attack," in *Beyond September 11th: An Account of Post-Disaster Research*, J. Monday (Ed.), Natural Hazards Research & Applications Information Center, Public Entity Risk Institute, and Institute for Civil Infrastructure Systems, Special Publication #39, University of Colorado, Boulder, CO, (2003), 165–198.
4. David Mendonça and W. A. Wallace, "Impacts of the 2001 World Trade Center Attack on New York City Critical Infrastructures," *Journal of Infrastructure Systems*, 12(4), (2006), 260-270.

Restoration *(Cont. from 12)*

banking) were statistically significant. A conclusion of this work, then, is that infrastructure interdependencies are highly relevant both to response and restoration work.

A number of specific examples illustrate how pre- and post-disaster infrastructure systems differ in form and function, whether in the short- or long-term. The following three have received considerable attention.

• Normal ferry service was suspended due to the ferries themselves being used to carry thousands of injured and other persons to New Jersey as part of an improvised waterborne evacuation. The ferry system is now an official component of the evacuation function with the emergency services infrastructure.[5]

• The destruction of two substations at the WTC complex, together with water main breaches in the vicinity of 7 World Trade Center, halted telecommunication service out of the Verizon building near Ground Zero, requiring considerable ad hoc rewiring of the building, coupled with the use of trailer-mounted diesel-fired electric power generators. Eventually the facility was returned to the electric power grid.[6]

• Telecommunication and power services to the New York Stock Exchange (NYSE) were severely compromised, perturbing world markets. Temporary power lines had to be run above ground, and trailer-mounted generators deployed to NYSE customers. Concurrently, power infrastructure managers "had to be careful to avoid the hoses that firefighters were running from the Hudson River to West Street." In other words, while work was underway, either firefighting equipment of power equipment could occupy the roads, but not both simultaneously.[7]

In these three cases, it may be seen how disasters may or may not provide opportunities for renewal of infrastructure systems. In the case of the ferry system, a private industry now serves as an adjunct to official emergency services.[8] In the telecommunications case, a new procedure — rewiring the building for power from the exterior — was developed, extending the scope of the organization's repertoire (i.e., a procedural change, not a material one).[9]

The electric power case merits further comment.[10] At a procedural level, much like the telecommunications case, the organization now has more extensive plans in place for deploying large numbers of trailer-mounted generators and for deploying temporary power lines over the road network. At the material level, it must be emphasized that, in the weeks and months following the attacks, engineers were actually constructing a new electric power distribution system, comprised of fewer networks than had existed before the attack. Moreover, the two substations previously located at the WTC were not restored (and may never be). Other smaller and larger changes have also been made to the system. Quite clearly, this disaster presented an opportunity to expand the organization's repertoire of procedures, but also to re-engineer its infrastructure.

Throughout our work — particularly within the telecommunications and power sectors — we were struck by the applicability of prior knowledge and experience to this very unusual event, and by the ability of personnel to adapt this knowledge to a very novel situation. The corporate knowledge bases were extensive, and informal communications were used to access it. In addition to the examples cited above are countless others from other organizations, both

(Continued on Page 31)

5. R. Pérez-Peña, "A Day Of Terror: The Government: Trying To Command An Emergency When The Emergency Command Center Is Gone," *New York Times,* New York, (2001), A7.
6. T. Pristin, "Phone Service Improving, but Many Still Lack Power," *New York Times,* New York, (2001), A12.
7. N. Banerjee, "Con Edison Crews Improvise as They Rewire a Truncated System," *New York Times*, New York, (2001), A14.
8. James M. Kendra, Tricia Wachtendorf, and E.L. Quarantelli, "The Evacuation of Lower Manhattan by Water Transport on September 11: An Unplanned Success," *Joint Commission Journal on Quality and Safety* 29(6), (2003), 316-318.
9. D. Mendonça, "Decision Support for Improvisation in Response to Extreme Events," *Decision Support Systems* 43(3), (2007), 952–967.
10. D. Mendonça, "Measures of Resilient Performance," in *Remaining Sensitive to the Possibility of Failure*, E. Hollnagel, C. Nemeth, S. Dekkers (Eds.), Ashgate Publishing Ltd., Aldershot, England, (2008).

The Evolving Focus on Securing the Transportation Systems Sector

by Irvin Varkonyi,
Adjunct Professor, Transportation Policy Operations and Logistics, George Mason University
School of Public Policy

Transport modes have played several different historical roles in the rise of civilizations (Egypt, Rome, and China), in the development of societies (creation of social structures), and also in national defense (Roman Empire, American road network).[1]

Transportation systems were at the heart of the tragedy on September 11, 2001. On that day, the U.S. passenger aviation system was the tool used by terrorists to take the lives of 3,000 people and drive a stake through the heart of the financial capital of the world. Even before that day, transportation systems were undergoing increasing stress. Capacity growth did not keep up with the demand for transportation capacity. Among the reasons were insufficient government investment in public sector owned assets; a lack of transportation planning at the national level; and poor earnings in the private sector which deprived the industry of sufficient capital for investments.

Thus, the lessons learned from the past decades of congestion and slow advances in environmental policy are now combined with the reality of terrorism in assessing transportation readiness and resilience. These lessons are reflected in the Transportation Security Administration's Transportation Systems Sector Specific Plan (TSSSP), first published in 2007 and updated in 2010.[2]

There have been significant changes in the TSSSP, most notably in the application of Systems Based Risk Management to protect the Transportation Sector. What are these changes and expectations in the continuing evolution of transportation systems? How well does the TSSSP move the dialogue for transportation systems security forward in addressing the concerns of industry stakeholders including corporate entities, industry associations, the government, and researchers? This article addresses these questions.

The Transportation Systems Sector

The Transportation Security Administration (TSA) and the U.S. Coast Guard (the maritime mode within the Sector) are the Sector Specific Agencies (SSAs) for the Transportation Systems Sector. The Postal and Shipping Sector is closely related, focusing on the small package industry. Indeed, postal and shipping has grown greatly over the past decade, resulting from the growth of internet business. There are differences between the Transportation Systems Sector and Postal and Shipping Sector, primarily based on their respective stakeholders. However, there are similarities in their system characteristics and risk management.

The TSSSP has developed strategies, among its stakeholders, to reduce risks to critical transportation infrastructure. Such infrastructure is composed of roads (highway or rural); rail (freight or passenger services); seaports (coastal or inland waterways); airports (commercial or general aviation); intracity mass transit systems; and pipelines, which cross thousands of miles of the Nation.

The TSSSP offers exhaustive views of each mode. It offers somewhat less attention on intermodal transport, the movement of goods or people seamlessly on a single freight bill or passenger ticket. Intermodalism has evolved rapidly since the advent of the shipping container by Malcolm McLean in

(Continued on Page 15)

1. Jean-Paul Rodrigue, Claude Comtois, and Brian Slack, *The Geography of Transport Systems*, 2nd Edition, Routledge Press, (2009).
2. U.S. Department of Homeland Security, *Transportation Systems Sector Specific Plan: An Annex to the National Infrastructure Protection Plan,* (2010).

Transportation *(Cont. from 14)*

1956. Cross modal risk assessments are described in the TSSSP as one of three classes of system specific risk assessments. Intermodalism's growth has been enabled by technology; transportation management systems are capable of handling moving goods without re-documentation as tracking systems are capable of showing complete movement regardless of modes utilized.

According to the 2010 Sector Specific Plan (SSP), it "revises the System Based Risk Management (SBRM) process described in the 2007 version of the SSP, and adopts and amplifies the National Infrastructure Protection Plan (NIPP) framework by describing a process intended to encourage wider participation in risk reduction decision making activities… Assessments may focus on a single risk factor or consider all three: threat, vulnerability and consequence."[3]

Transportation Stakeholders

Transportation systems are composed of private and public sector entities. U.S. based airlines, truckers, and freight rail are privately owned. Maritime companies are a mix of private and public with the latter principally owned by governments in Asia and Europe. Seaports and airports are also a mix of private firms and various government entities including, Federal, State, county, and city agencies. Pipelines are privately owned. Government is inextricably intertwined with the Transportation Systems Sector because of safety and security regulations, which provides the government with the ability to direct security compliance.

Transportation is dependent on government's financial support. For example, the highway industry is dependent on massive Congressional legislation such as the Safe Accountable Flexible Efficient Transportation Equity Act (SAFETEA-LU). The Act, passed in 2005, follows up earlier transportation re-authorization legislation. It established $244 billion for enhancement and improvements in surface transportation investment. At the time, it was the largest transportation investment for the Nation.

There is new re-authorization legislation in Congress; however, current government spending appears to spell far lower investments for highways than requested by industry stakeholders. However, on an interesting note, the American Society of Civil Engineers *Report Card for America's Infrastructure* (2009) rated U.S. transportation infrastructure as a "D." It estimated that $2 trillion dollars of investment were needed to improve infrastructure and build new infrastructure to meet expected demand through the next decade.[4]

Security and Safety

Transportation also inextricably combines safety and security missions. Government oversight of hazardous materials establishes standards for transportation companies, their personnel, and the assets used to mitigate accidents. Such mitigation has become more complex since the movement of hazardous materials may also be used as a tool to intentionally cause catastrophic incidents. It may be difficult to discern terrorist acts from accidental disruptions. The TSSSP must deal with this complexity and uncertainty on the causes for hazardous materials incidents. These issues are captured in the TSSP's Development of Protection and Resiliency Priorities. Some of the notable issues involve:

- Safety/Security Conflicts
- Transportation Flow (congestion mitigation)
- Unfunded Mandate Issues
- Competing National Budget Priorities

The TSSSP offers four goals to achieve the mission of securing transportation systems:

1. Prevent and deter terrorism;
2. Enhance the all-hazard preparedness and resilience of global transportation systems;
3. Improve effective use of resources for transportation security; and

(Continued on Page 16)

3. Ibid.
4. American Society of Civil Engineers, *2009 Report Card for America's Infrastructure*, (2009), http://www.infrastructurereportcard.org/sites/default/files/RC2009_full_report.pdf.

Transportation *(Cont. from 15)*

4. Improve sector situational awareness, understanding and collaboration

Transportation is ubiquitous. From unrestricted movement of commuters riding the Washington Metro to severely congested highways on New York's Long Island Expressway to an endless line of trucks waiting for containers at the Los Angeles/Long Beach seaport, transportation is the lifeline for the American economy. It must overcome system stress. Consider the vulnerability of pipelines in North America, which traverse States and provinces without a single human living within hundreds of miles of pipelines. Transportation is everywhere. Thus, the TSSSP seeks to utilize SBRM to rationalize limited resources and risk mitigation. In some areas, the government seeks 100 percent certainty, such as screening of all passengers traveling commercial airlines flights within the United States as well as internationally. The 100 percent screening of air cargo moving on passenger aircraft also seeks a 100 percent solution.

An All-Hazards Approach

TSA invests heavily in its "Capability Gap Process," a tool used to develop detailed risk based needs. Many of these are performed in common with all of the 18 critical infrastructure sectors — entry and access portals, insider threats, response and recovery tools, and more. The private sector stakeholders must deal with the risks of potential terrorists; however, they have more concerns beyond terrorism to consider which may cause disruptions. Among these are included:

- Cargo theft
- Smuggling of contraband
- Smuggling of human cargo
- Hazardous materials accidents
- Congestion of transport modes
- Financial instability
- Excessive vulnerability to fuel price volatility

The threats faced by transportation systems are extensive. The TSSSP offers guidance to assess risks based on the probability and consequents of perceived threats. An additional tool that needs to be incorporated in decision-making is a process to trade off risk mitigation with operational imperatives. Where is that proverbial "sweet spot," to find the right balance? As in any operation, transportation systems must optimize operational efficiency while they simultaneously minimize operational vulnerability.

Transportation is not limited to a geographically defined sector as are many other of the 18 sectors. It is a global system operating under multiple regulatory bodies, geographical diversity, and financial inequities of government owned systems vs. privately owned systems. The TSSSP focuses on U.S. based transportation systems but this industry operates globally. After all, vulnerability is not limited to U.S. based operations. Consider terrorism on the Madrid railroad in 2004 and increasing maritime piracy off the coast of Somalia, or terrorist explosions in the Moscow underground and the near success of the smuggled bomb inside office equipment sent from Yemen, both in 2010.

These situations illustrate the vulnerabilities of the transporation system. As quoted by a popular textbook, "[t]he ideal transport mode would be instantaneous, free, have an unlimited capacity and always be available. It would render space obsolete. This is obviously not the case. Space is a constraint for the construction of transport networks. Transportation appears to be an economic activity different from the others. It trades space with time and thus money."[5]

Transportation will always be vulnerable to all manners of disruptions and threats. An integrated approach to securing transportation systems offers the most reasonable prospects for success.

Conclusion

Transportation has many stakeholders throughout the private and public sectors. Transportation systems are stressed due to many factors, of which terrorism is but one. These systems are vital to the Nation's economy. Yet the resources to modernize transportation are stressed by the state of the economy and by the state of the Federal budget. Transportation is not

(Continued on Page 28)

5. *Transportation Geography – What Do I Know?* Press Universitaires de France, 1992.

Control System Cybersecurity – An Anthology since 9/11

by Joe Weiss, PE, CISM, CRISC, ISA Fellow, IEEE Senior Member*

Industrial Control Systems (ICSs) operate the industrial infrastructures world-wide, including electric power, water, oil/gas, pipelines, chemicals, mining, pharmaceuticals, transportation, and manufacturing. ICSs measure, control, and provide a view of the process (once only the domain of the operator). ICSs include Distributed Control Systems (DCS), Supervisory Control and Data Acquisition Systems (SCADA), Programmable Logic Controllers (PLCs), Remote Terminal Units (RTUs), Intelligent Electronic Devices (IEDs), and other field sensors and controllers. From a security perspective, ICSs were generally isolated networks and the concept of "security by obscurity" was alive and well. In fact, papers on the "evils of islands of automation" and the need to integrate the various systems were being written by this author. As security was not a consideration, there was little reason to question the need for tighter system integration. However, these systems continue to be upgraded with advanced communication capabilities and networked to improve process efficiency, productivity, regulatory compliance, and safety which make them vulnerable to cyber impacts. This networking can be within a facility or even between facilities continents apart. When an ICS does not operate properly, it can result in impacts ranging from minor to catastrophic. Consequently, there is a critical need to ensure that electronic impacts do not cause, or enable, misoperation of ICSs.

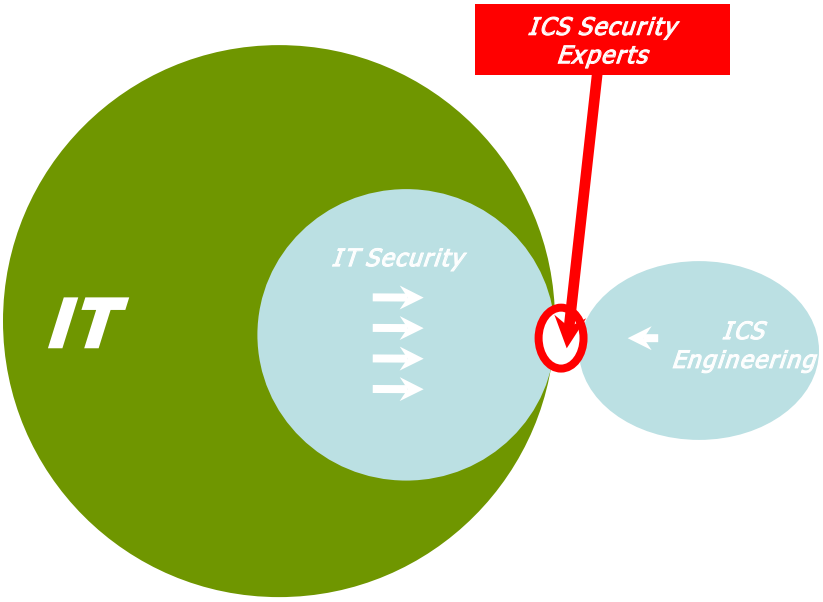

Figure 1: ICS Security Expertise Lacking

Security is like a three-legged stool, consisting of physical security, IT security, and ICS security. Physical security is generally well-understood and often addressed by experts coming from the military or law enforcement. IT security generally deals with traditional commercial off-the-shelf (COTS) hardware and software and connections to the Internet with experts from IT and the military. There is little doubt that IT security is necessary and that systems are continuously being probed, tested, and hacked. The third leg, ICS security, is much less understood, has little expertise, and is often not considered critical. Those working in this area are generally either from the IT security community with little knowledge of ICSs or ICS experts knowledgeable in the operation of systems, but not security. From a cybersecurity perspective, ICSs and IT are very different; therefore, the same technologies, training, policies, and testing may not be directly applicable. The cybersecurity vulnerabilities of the COTS (Windows) interface and Internet Protocol (IP) communication vulnerabilities are generic issues being addressed by the general IT security community. However, only the ICS community will address the cyber vulnerabilities associated with ICS communications, ICS protocols, and ICS systems.

(Continued on Page 18)

Cybersecurity *(Cont. from 17)*

Furthermore, these vulnerabilities have generally not been addressed because they are not well-understood by the IT community. Unfortunately, these vulnerabilities have already been exploited by Stuxnet and the Aurora test performed by the Idaho National Laboratory. Protecting ICSs is indeed "rocket science" because the ICS must continue to perform its function when security is actually trying to inhibit the systems form doing so. Consequently, ICSs can, and have, already been impacted by cyber threats. Figure 1 (see page 17) provides a view of the need to educate more people in control ICS cybersecurity as there are arguably only several hundred people that truly understand ICS cybersecurity.

Background

In the 1997 time-frame, the Y2K issue finally made it to the ICS community. Y2K was an unintentional cyber issue focusing on the ability of digital systems clocks and Basic Input/Output Systems (BIOS) to account for the century change. With the focus on Y2K, it left very little room for addressing more traditional cyber threats. However, there were two issues involved with the Y2K situation that, at the time, did not appear consequential but have since had a significant impact on cybersecurity of ICS. The first issue was a negative impact. There was significant money spent on Y2K with little "apparent" resulting impacts. Instead of viewing the Y2K program as a success by preventing mass impacts, most senior managers viewed the lack of impact as an indication it was nothing but FUD — Fear, Uncertainty, and Doubt — created by the vendors and consultants to sell their wares. Many in senior management continue to harbor the perception that ICS security is like Y2K — that is FUD. This is hurting the industry very badly. The second issue with Y2K was a positive impact. Y2K created an once-in-a-lifetime environment of information sharing within each company and between companies. Unfortunately, we did not realize it was an once-in-a-lifetime event. When the ICS Cyber Security Program started at EPRI in early 2000 (actually called the Enterprise Infrastructure Security Program), we expected the same level of information sharing to occur as occurred during Y2K. Were we ever wrong! In retrospect, there were different drivers between Y2K and ICS security. The biggest was liability. For Y2K, officers and directors were personally liable. It was no wonder they took it so seriously. The same liability issue has not been applied to ICS security.

ICS cybersecurity was formally identified in the mid-late 1990s with the publication of PDD-63.[1] It was at this time that the U.S. Department of Energy's (DOE) National Laboratories starting performing cybersecurity assessments of utilities on a confidential (not classified) basis. As these assessments were not made public, there was little knowledge of the results unless the utilities' were willing to share their results.

Various industries started to address cybersecurity in the mid-to-late 1990s. In 1999, the Gas Technology Institute (GTI) initiated development of gas SCADA communication protection systems. The premise was that the cyber weak link was the communications between the remote terminal unit (RTU) in the field and the SCADA system. The Chemical Industry had formed Chemical Industry Data Exchange (CIDX) in the mid 1980s and used that vehicle to start to address cybersecurity in the late 1990s.

Other industries such as water and petroleum also started efforts to address cyber security in the late 1990s and early 2000s. The electric industry initiated efforts in March 2000 (this author was the technical lead). At the time, ICS cybersecurity awareness in the electric industry was very low and its perceived importance even lower. Generally, it was viewed as a corporate IT issue with little direct impact on power plant or grid operation. Moreover, it was viewed as a hindrance to ICS technology advancements.

When the ICS Cyber Security Program first started at EPRI in early 2000, cybersecurity was not viewed as a national security imperative by private industry. ICS security was viewed as a business issue since ICS systems were critical to the "bottom line" of an industrial company. In fact, on September 10,

(Continued on Page 19)

[1] Presidential Decision Directive (PDD)-63, May 22 (1998), http://www.fas.org/irp/offdocs/pdd/pdd-63.htm.

Cybersecurity *(Cont. from 18)*

2001, two panel sessions on ICS Security were held at ISA Expo in Houston, TX. Attendees included representatives from electric utilities, water, oil/gas, and pipelines. Attendees also included auto parts manufacturers and even a dog food manufacturer. The next day, the world changed forever. From that infamous date onward, the perception of ICS security changed from a business issue to a national security imperative. This had the unfortunate implication of the onus being shifted from the end-user to the government.

There was one other item that, at the time, seemed perfectly reasonable, but in hindsight, has been very disruptive to securing the efficient operation of ICSs. That item was the name "Cybersecurity." Little did we realize the difference it would have made if we had used the term Critical Infrastructure Protection, Functional Security, or Control System Electronic Communication Reliability. By calling the issue cybersecurity, the focus was transferred from maintaining control system and process reliability, regardless of computer status under the aegis of the operations organization, to focusing on computers regardless of control system and system reliability under the aegis of the IT organization.

Cybersecurity is not limited to the SCADA or DCS human-machine interface but extends throughout all of the system interconnections. The Stuxnet worm makes this very clear as this was an attack on the PLC logic and the Windows interface was only used as a vehicle for transmitting the "warhead" to the PLC.

When ICS cybersecurity began, most people were not aware of ICSs; therefore, most systems were simply out of the cybersecurity scope. In the 2005 time frame, the North American Reliability Council (NERC, now North American Reliability Corporation) issued the first version of the NERC Critical Infrastructure Protection (CIP) guidelines. The CIP guidelines were the first industry cybersecurity guidelines with oversight (audit) requirements. These standards were generated by the industry and included various exclusions. The NERC CIPs have done a great service to the industry in making cybersecurity more evident. However, there are several downsides:

- All systems not specifically included in the CIP scope effectively have no cybersecurity program.
- The NERC CIPs do not require ICS cybersecurity training. Consequently, most people involved are not domain experts of the systems ostensibly being secured.
- Given that the CIPs are programmatic, they have spawned an industry to address the compliance issues but have inadvertently discouraged development of ICS security technology.

Why Care

The fundamental reason for securing ICSs is to maintain the mission of the ICSs, be it to produce or deliver electricity, make or distribute gasoline, provide clean water, etc. in a safe and efficient manner. Since 1999, there have been more than 200 actual control system cybersecurity unintentional incidents and malicious cyber attacks. The impacts range from trivial damage to significant environmental and equipment damage to major electric outages to deaths. Many of these incidents appear to be recurring, yet there is minimal and sometimes conflicting guidance to the end-user. There are minimal ICS cyber forensics so the vast majority of the incidents were not identified as "cyber." Stuxnet was arguably the first nation-state stack against infrastructure. It was in the wild for more than a year before it was found. There is still minimal guidance to the end-user on how to detect the warhead and little Research and Development (R&D) addressing the field devices such as PLCs that can cause the greatest harm. Moreover, the publicity associated with Stuxnet has spawned the development of cyber attack tools against these critical ICS systems now available on the net. It is no longer necessary to be a nation state to attack these systems, making resilience and recovery even more important.

What Still Needs to be Done:

- Develop a clear understanding of ICS cybersecurity. This includes developing a clear understanding of the associated impacts on system reliability and safety on the part of

(Continued on Page 31)

Interview with Virginia State Trooper Michael Middleton: Lessons Learned in Law Enforcement since September 11, 2001

On September 11, 2001, the largest assault on U.S. soil since the devastating surprise attack on Pearl Harbor in 1941 began when American Airlines Flight 11 crashed into the North Tower of the WTC in New York City. Approximately 20 minutes later, as the confused media and public struggled to determine the cause of the crash, the deafening roar and the dark shadow of United Airlines Flight 175 loomed overhead. As realization dawned that America was under attack, almost 30 minutes later, American Airlines Flight 77 struck the western side of the Pentagon in Arlington, Virginia. Trooper Michael Scott Middleton, a 15 year veteran of the Virginia State Police this October, was working traffic on the Dulles Toll Road and Eastbound 66 when the third plane crashed into the Pentagon. We had the honor of speaking with Trooper Middleton about his experience that day as well as the lessons learned in law enforcement since the world was forever altered ten years ago.

On the morning of September 11, 2001, Trooper Middleton was working routine traffic stops on the Dulles Toll Road when a colleague informed him that a plane had crashed into the North Tower of the World Trade Center. As he listened to WTOP radio, he, along with a majority of the Nation, deduced that the crash was most likely attributed to "pilot error." However, once it was revealed that a commercial airliner as opposed to a small aircraft was involved, he "started feeling a little uncomfortable." At this point, he decided to drive to the area office in Arlington to turn on the news and find out more about the alleged accident.

As he navigated his way towards the office, Trooper Middleton made a routine traffic stop at the interchange of the Dulles Toll Road and Eastbound 66. He was in the middle of writing the ticket when he heard that a plane had struck the Pentagon. After quickly returning the license and registration of the driver, he raced down Eastbound 66 towards the Pentagon. Ten years later, he still remembers "coming off route 110, and just seeing this huge mushroom cloud of fire and smoke pointing up into the sky. I remember getting off the Pentagon exit, and you could see the impact … I remember getting on scene, rushing directly to the site where the plane had hit."

After Trooper Middleton arrived on scene, he searched for Merlin Wimbush, a fellow State Trooper who was working at the Arlington office when the plane struck the Pentagon. As Trooper Middleton describes, "I just remember getting on scene. I ran into a Pentagon Police Officer; he said that the trooper [Merlin Wimbush] went inside, and that's when I went in… it was pitch black, and there was smoke, I remember the thickness of the smoke." After locating Trooper Wimbush through the fog of smoke, the next thing he remembers "was standing at ground zero… it was pure hell, it was like I was in hell itself."

For the next several minutes, Trooper Middleton, along with Trooper Wimbush, Pentagon Police Officer Donald Behe, and another individual, searched for survivors. When asked how long he was in the Pentagon, he answered, "To me, it felt like an eternity, like I was in there for hours, time was moving slowly. Maybe 20 minutes, I don't really recall, it wasn't too long." After running into fire and rescue on the fourth floor, Trooper Middleton, who was not wearing protective gear, and his fellow rescuers were encouraged to exit the building. At this point, he began to feel the intense, dizzying affects of the fire and smoke without the protection of a mask. As soon as he exited the building, he finally succumbed to the smoke and fire and briefly lost consciousness.

Shortly thereafter, Trooper Middleton was treated in the parking lot of the Pentagon. While he was being treated, "a voice screamed though the parking lot, 'get him the hell out of here, there is a plane inbound, and it's supposed to crash here again.'" From the

(Continued on Page 21)

Law Enforcement *(Cont. from 20)*

parking lot, he was swiftly thrust into an ambulance and transported to Inova Alexandria Hospital. For the next several days, Trooper Middleton drifted in and out of consciousness as he was treated for smoke inhalation and first and second degree burns. His condition drastically worsened when he developed sepsis (blood infection), pneumococcal pneumonia, and acute respiratory distress syndrome, during the next two or three days. While Trooper Middleton's recollection about this period of his life is hazy, he claims that his "20 minutes in the Pentagon was nothing compared to what my wife went through for a week of seeing her husband in an induced coma with tubes in him." However, his wife was not the only person concerned for him and other victims being treated at the hospital. At one point, he was rushed to the operating room and "she [wife] said that when I came out, down the hallway was lined with doctors and nurses, and they were all holding flags." Miraculously, Trooper Middleton returned to work on November 1.

As the conversation turned to the impact of September 11 on emergency response, Trooper Middleton began to discuss the evolution of law enforcement in the last ten years. Needless to say, changes to law enforcement education and training in emergency response have been significant in the last decade. As Trooper Middleton pointedly remarked, on the morning of September 11, "[n]obody was prepared for that day. On that day, we were law enforcement, first responders on the scene who did what we had to do. Anybody on the scene, like myself and Trooper Wimbush, we were doing instinctively what we were trained to do and what we knew had to be done which was search for survivors." Indeed, Trooper Middleton replied that the most challenging aspect of that day, in terms of logistics and response, was chaotic traffic and unpreparedness. As he stated, "generally I would have to say traffic. Traffic was so discombobulated that day. But, I'd say the biggest thing was probably unpreparedness…not just the State police, but also on my part because I really did not have a clue what I was doing when I got down there. I was going on full adrenaline, full fear, full anger...That's when law enforcement training kicked in; I kept saying, stay focused, stay focused, do your job, do what you gotta do."

Prior to September 11, his training consisted primarily of basic, albeit intense law enforcement training. While Trooper Middleton did receive additional training as a member of S.W.A.T. from 2004 to 2009, prior to 2001, Virginia State Police officers were required to endure "26 weeks of intense training." However, in the wake of September 11th, Virginia State Troopers have increased their education and training in self-awareness, particularly of surroundings, and emergency response. In other words, officer safety has improved, particularly with regards to suspicious persons. For example, he explained, "[w]hen I went to the academy, we received basic training about bank robbers and such, but now there is a list that you have. If you think you have encountered a possible terrorist, there are certain steps and procedures that you have to take and follow. It is no longer walking up to a car, [asking for] license and registration, and here's your ticket. Now, you are walking up to the car, looking around the car, paying attention, looking around vigilantly. Do I see things? Do I see maps in the car? Is there camera equipment in the car?"

In addition to increased training in self-awareness, State law enforcement officials are now required to take specific online courses. The content of the courses, he said, is determined by law enforcement leadership. For example, he recently took a course on cyber awareness and internet security. Furthermore, law enforcement officials are equipped with better resources through Federal funding and grants. According to Trooper Middleton, when he first reported for duty 15 years ago, his department did not have gas masks. Additionally, his department had the oldest radio in the State. Now, he said, his department has better equipment, better weapons, better materials, and better resources than it did 15 years ago. He continued, "[s]omething else that changed was flashlights. They got rid of battery flashlights, and now they use rechargeable flashlights. So, things have changed, things have

(Continued on Page 22)

Law Enforcement *(Cont. from 22)*

advanced." With more resources and improved planning and training, "now we get out of the car, grab the gas mask, grab the flashlight."

When he was asked if there is still a need for improvement in response and planning, he responded, "[t]hat's true always. There are things we are doing that I am not at liberty to discuss, but what I can say is that our department, as well as other agencies, are always preparing. Since 9-11, a lot of agencies have realized that we need to work diligently together for better preparedness." This is especially true with regards to evacuation, a subject that has received significant attention in the aftermath of September 11.[1] As Trooper Middleton elaborates, "[o]ne of the biggest questions that came up, that still comes up, is evacuation. How to evacuate somebody if there is a 9-11. What if they blew up the bridges? You need an evacuation plan. We work with the Virginia Department of Transportation and engineers. We also think about how to clear the area and better secure the area if there is a terrorist cell we need to take down."

Trooper Middleton stated that one of the biggest lessons learned from that day was the realization that law enforcement needed more training in preparedness and response. As he stated, "[I] can honestly say I feel that my department is really striving for their best to keep us prepared, keep us informed, and keep us better equipped, so that if God forbid there is another event like 9-11, we will have a better opportunity to have a higher survivability rate, getting people to a safer area and out of the way of harm."

Perhaps most importantly, Trooper Middleton said that his department is working with DHS and other Federal agencies. According to him, his department is working "hand-in-hand with the Federal government and other agencies." Prior to September 11, he said, "everybody was their own department, Fairfax, Alexandria, and so forth." For example, ten years ago, there was no real communication between the different departments. Now, however, there is much more sharing of information. This, he said, demonstrates more connection between the departments. However, as always, there is still room for improvement. When asked if the different agencies and jurisdictions are working better together now, he said, "[I] would say, yes. Is that to say 100% we are working together? There is still some gun shyness, I'm sure, but that's not just in law enforcement."

When asked if he feels better prepared to face another incident like September 11, he answered the question with a reference to the topic of this month's issue: lessons learned. He replied, "[t]en years ago, you [in reference to the interviewer and the media in general] would hear about the attack, and you would just want to report it, just the devastation of the attacks at the Pentagon and in Pennsylvania and New York, and that's it. Well, now you have folks like yourself who want to talk about the changes with [regards to] preparedness as well as lessons learned…asking what they [law enforcement and emergency responders] have accomplished and where we are going in the future. So, your preparedness is also helping us." In other words, increased education and training and studies in lessons learned have ensured that emergency responders are at the very least better prepared to respond to an incident similar to September 11.

In the ten years since September 11, Trooper Middleton has continued to serve his country and his constituents as a Virginia State Trooper. He has been involved with numerous challenging and grueling situations, such as the 2002 sniper attacks in Maryland, Virginia, and

(Continued on Page 32)

1. For example, see studies by Rae Zimmerman and Martin F. Sherman, "To Leave an Area After Disaster: How Evacuees from the WTC Buildings Left the WTC Area Following the Attacks," *Risk Analysis*, 31(5), (May 2011), 787-804; N.C. McConnell, K.E. Boyce, J. Shields, E.R. Galea, R.C. Day, and L.M. Hulse, "The UK 9/11 Evacuation Study: Analysis of Survivors' Recognition and Response Phase in WTC1," Fire Safety Journal, 45(1), (January 2010), 21-34; R.G. Gann, *Final Report of the Collapse of World Trade Center Building 7*, *Federal Building and Fire Safety Investigation of the World Trade Center Disaster* (NIST NCSTAR 1A), National Institute of Standards and Technology, (November 2008); and Robyn R.M. Gershon, Marcie S. Rubin, Kristine A. Qureshi, Allison N. Canton, and Frederick J. Matzner, "Participatory Action Research Methodology in Disaster Research: Results From the World Trade Center Evacuation Study," *Disaster Medicine and Public Health Preparedness*, 2(3), (October 2008), 142-149.

September 11, 2001 Memorials

On the morning of September 11, 2001, terrorists hijacked four planes and took the lives of over 3,000 innocent people, including children. As is etched into the hearts and minds of millions of people around the world, two planes crashed into the North and South Towers of the WTC in New York City, NY; one plane crashed into a field in Shankesville, PA; and one plane crashed into the Pentagon in Washington, D.C. To pay tribute to the innocent lives lost, memorials have been erected at each location for reflection and remembrance.

The National September 11 Memorial Museum at the World Trade Center

At 8:47a.m., American Airlines Flight 11 crashed into floors 93-99 of the World Trade Center's North Tower. Almost 20 minutes later, at 9:03a.m., United Airlines Flight 175 crashed into floors 77-85 of the World Trade Center's South Tower.

On September 11, 2011, the National September 11 Memorial Museum at the World Trade Center will be dedicated. The 9/11 Museum will open the following year. The National September 11 Memorial and Museum at the World Trade Center Foundation, Inc., a non-profit, was created to oversee construction and maintain the monument. The Port Authority of New York and New Jersey (PANYNJ) is the construction manager for this memorial.[1]

The memorial pays tribute to all of the victims of the 9/11 attacks at the WTC, the Pentagon, and in Pennsylvania, as well as the victims in the 1993 WTC attack. Where the twin towers once stood, there will be twin reflecting pools and they will "feature the largest manmade waterfalls in North America."[2] The names of everyone who perished in the 1993 and the 2001 attacks are engraved into bronze panels that line the memorial pools. This will serve as a reminder "of the largest loss of life resulting from a foreign attack on American soil and the greatest single loss of rescue personnel in American history."[3]

For additional information on this memorial, please visit http://www.911memorial.org/.

A Memorial Unit at the Pentagon Memorial; a cantilevered bench, a glowing pool of light, and a permanent tribute, by name, to each victim. *Photo courtesy of Elizabeth Hale-Salice.*

The Pentagon Memorial

At 9:37a.m., American Airlines Flight 77 crashed into the first floor of the western façade of the Pentagon. One-hundred-and-eighty-four people perished on board Flight 77 or in the Pentagon.

(Continued on Page 33)

1. http://www.911memorial.org/about-us-0.
2. http://www.911memorial.org/about-memorial.
3. Ibid.
4. http://pentagonmemorial.org/about-us.
5. http://pentagonmemorial.org/explore/interactive-map.

United States Senate Committee on Homeland Security and Governmental Affairs Hearing
Ten Years After 9/11: Preventing Terrorist Travel

On July 13, 2011, the Senate Committee on Homeland Security and Governmental Affairs held a hearing to review the state of our Nation's terrorist defenses as we approach the 10th Remembrance of September 11th. The Honorable Rand Beers, Under Secretary, NPPD, DHS; the Honorable Janice L. Jacobs, Assistant Secretary, Bureau of Consular Affairs, U.S. Department of State; and the Honorable David F. Heyman, Assistant Secretary, Office of Policy, DHS, provided their testimonies. Although significant progress has been made, terrorists continue to adapt. Agencies must look for innovative ways to bridge the gaps in intelligence, information-sharing, technology, and decision-making.

To read the testimonies and/or view the archived webcast, please visit http://hsgac.senate.gov/public/index.cfm?FuseAction=Hearings.Hearing&Hearing_ID=af5eac3a-fe02-493e-89ea-64fab7c88259.

Presidential Policy Directive/ PPD-8: National Preparedness

On March 30, 2011, President Barack Obama signed PPD-8, superseding HSPD-8: National Preparedness and HSPD-8 Annex 1: National Planning (with the exception of paragraph 44). PPD-8 seeks to improve the security and resilience of this Nation against threats such as terrorism, cyber attacks, pandemics, and catastrophic natural disasters. It seeks to accomplish this mission by developing a national preparedness goal that identifies the "core capabilities" of all levels of government, the private and non-profit sectors, and individual citizens required for effective preparedness.

In order to meet this goal, the Secretary of Homeland Security has been mandated to establish a national preparedness system, or an "integrated set of guidance, programs, and processes." However, to ensure that the national preparedness system embraces an "all-of-Nation" approach, the Secretary has been directed to develop a comprehensive outreach strategy. Finally, the directive assigns roles and responsibilities, defines relative terms, including the term "resilience," and states that a report must be submitted on March 30, 2012.

In August 2011, a draft of the national preparedness goal was released by the Federal Emergency Management Agency for comments. An electronic copy of the draft is available at http://www.fema.gov/pdf/prepared/npg.pdf. It is most notable for its description of the Strategic National Risk Assessment and its extensive list of core capabilities and performance objectives.

This directive is particularly salient given that September is National Preparedness month. Indeed, as the world prepares to honor the victims and heroes of the September 11 attacks; the unprepared residents of the U.S. East Coast recover from the shock of a historic 5.8 magnitude earthquake; and at the time of this writing, prepare for the wrath of Hurricane Irene, the "all-of-Nation" message of this directive could not be timelier. In order to improve the security and resilience of this Nation, it essential that Federal, State, local, tribal, and territorial governments collaborate with the private sector as well as the individual citizen to enhance emergency preparedness and response and personal resilience.

For more information, please see http://www.dhs.gov/xabout/laws/gc_1215444247124.shtm.

Legal Insights

The Changing Legal Regime in Post 9/11 America

In the ten years that have passed since September 11, an array of laws and regulations have been implemented to shore up perceived gaps in the pre-9/11 legal regime and to help America meet the security needs of a post-9/11 world. The connection between securing the homeland and securing critical infrastructure was noted by Joe D. Whiteley, the first General Counsel of DHS, who said that "[a]rguably the defense (and, if necessary, the rapid reconstitution) of these critical infrastructures and key assets sectors is homeland security."[1] This month's *Legal Insights* will provide a brief overview of some of the major regulations and laws that have passed since September 11 that have focused in whole or in part on critical infrastructure protection.

Homeland Security Act of 2002

The Homeland Security Act was passed on November 25, 2002. This act significantly transformed the landscape of homeland security by combining 22 separate Federal agencies under the umbrella of the newly created Department of Homeland Security. One of the most important provisions of this act relating to critical infrastructure was found in Title II Subtitle B, known as the Critical Infrastructure Information Act of 2002. This Act created the Protected Critical Infrastructure Information Program and amended the Freedom of Information Act (FOIA). This program and legislation allowed critical infrastructure owners and operators to share information related to homeland security with the Federal government while having that information protected from FOIA disclosure.

Transportation Systems Sector

The nature of the 9/11 attacks demonstrated the vulnerability of many transportation vectors to be attacked and to be used as a weapon. As a result, a number of laws were passed which attempted to secure the Transportation Systems Sector. The first law that was passed was the Air Transportation Safety and System Stabilization Act, which provided economic support to the aviation industry. This was then followed by:

- The Aviation and Transportation Security Act of 2001, which established the Transportation Security Administration within the Department of Transportation as an agency responsible for security in all modes of transportation and authorized the use of Federal air marshals on all passenger flights

- The Maritime Transportation Security Act of 2002 was passed in November 2002 to increase the security of ports. This act was estimated to directly affect "10,000 vessels, 5,000 facilities and 40 outer continental shelf facilities" and requires security assessments and development and implementation of security plans.[2]

- The Pipeline Safety Improvement Act of 2002 aimed at improving pipeline security, a component of the Transportation Systems Sector, by improving pipeline operation, leak and damage prevention, and monitoring and control systems.[3]

- The Security and Accountability for Every (SAFE) Port Act was passed in 2006. In 2005, the Domestic Nuclear Detection Office was created by a Presidential Directive with the goal of preventing radiological and nuclear attacks. The SAFE Port Act established this office in statute and required it to develop "an enhanced global nuclear detection architecture." The act also bolstered general requirements for container

(Continued on Page 26)

1. http://www.atlanta-businesslitigation.com/Homeland-Security-Law-Policy-Jurimetrics.pdf.
2. www.aapa-ports.org/files/PDFs/mtsa_press_kit.pdf.
3. http://www.enewsbuilder.net/aopl/e_article000502826.cfm.

Legal Insights *(Cont. from 25)*

security, including a provision to scan all containers entering high-volume ports for radiation sources and codified two more existing programs, the Container Security Initiative (CSI) and the Customs-Trade Partnership Against Terrorism (C-TPAT). The CSI is a partnership between the U.S. government and foreign governments while the C-TPAT is a partnership between the U.S. government and private enterprise. Both are aimed at increasing the safety of trade and are discussed in greater detail in the December 2010 issue of *The CIP Report*.[4]

Other Sectors

In addition to the heavy emphasis on the Transportation Systems Sector, other laws were passed which focused on cross-sectoral emphasis, such as information sharing and additional sectors. Among these laws are:

- The Public Health Security and Bioterrorism Preparedness and Response Act of 2002 was passed to promote the cooperation of Federal, State, and local partners in responding to a bioterrorism event and to improve reporting mechanisms, enhance laboratory readiness, ensure the availability of a properly trained workforce, maintain appropriate communication to the public/private sector and to the public at large, and to maintain an adequate stockpile of drugs, vaccines and other pharmaceutical devices.[5]

- The Energy Policy Act of 2005 created minimum "mandatory standards of reliability for the U.S. energy sectors" to secure the availability of electric power.[6]

- The Implementing Recommendations of the 9/11 Commission Act was passed in 2007. The critical infrastructure legislation contained in this act was extensive but generally pertained to two sectors, Emergency Services and Transportation Systems. It also referred to the general concept of information sharing. Title II of the act authorized grants for emergency management and Title III was focused on providing for interoperability of communications for first responders. The emphasis on information sharing extended throughout other Titles of the act, including Title V, which focused on integrating information across Federal, State, local, and tribal governments. The other major emphasis of the act was on the Transportation Systems Sector, which was specifically addressed in 7 of the 24 Titles of the act, including provisions specific to public transportation, railroads, airways, and maritime cargo.

Regulations

One of the most prominent regulations to arise from DHS related legislation is the Chemical Facility Anti-Terrorism Standards (CFATS) interim rule that was promulgated under the authority of the Homeland Security Appropriations Act of 2007. CFATS establishes "risk-based performance standards" to secure chemical facilities and plays a role in the chemical, critical manufacturing, energy, nuclear reactors, materials and waste, and water sectors.[7]

Presidential Directives

- On December 7, 2003, HSPD-7, Critical Infrastructure Identification, Prioritization, and Protection, was issued by the Bush Administration. This directive established "a national policy for federal departments and agencies to identify and prioritize U.S. critical infrastructure and key resources and to protect them from terrorist attack."[8] The NIPP meets the requirements of HSPD-7 and sets forth "a comprehensive risk management framework and clearly defined roles and responsibilities."[9]

- On January 30, 2004, HSPD-9 was issued. This directive established "a national policy to

(Continued on Page 27)

4. *Nuclear Detection Domestic Nuclear Detection Office Should Improve Planning to Better Address Gaps and Vulnerabilities*, GAO, January 2009.
5. http://thomas.loc.gov/cgi-bin/bdquery/z?d107:HR03448:@@@D&summ2=m&.
6. http://www.nu.com/responsible_energy/our-business/reliability.html
7. http://www.dhs.gov/files/laws/gc_1166796969417.shtm.
8. http://www.dhs.gov/xabout/laws/gc_1214597989952.shtm.
9. http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf.

Uncertainties *(Cont. from 3)*

high corporate tax rates, nationalizing all issues, and currying favor with special interests are not helpful. Whether correct or not, these perceptions influence attitudes toward government and cannot help but affect the level of cooperation between citizens, businesses, and government.

As business entities have gone through the process of "right sizing" to survive and maintain profitability during this long, flat economic recovery, their focus on protecting assets has probably never been higher. Is the private sector — all six million businesses with employees —really concerned with potential losses to terrorism? Perhaps some are, but for the most part, businesses today are making risk calculations based on current economic conditions, and terrorism is simply one more aspect to be included in determining what protective measures need to be deployed.

As technology advances and more and more businesses become dependent on cyberspace, reducing uncertainty and mitigating risk become increasingly problematic. Can businesses and citizens depend on government to protect them, or must citizens become more self-reliant? Given the level of trust and confidence people have in government today, one should hope that moving our culture to one of greater individual self-reliance might have positive consequences.

Reflecting back on the unity of purpose found in this Nation in the wake of the 9/11 terror attacks, one is struck by how little cohesion there seems to be between the citizens of the Nation and the government today. If this loss of innocence and confidence in government are the new reality, then the re-emergence of robust, self-reliant citizens and cautious, focused businesses might be the most positive, though unintended, consequences of the evolution of this Nation over the interceding ten years. ❖

Legal Insights *(Cont. from 26)*

defend the agriculture and food system."[10] This directive required heads of certain Federal departments and agencies to develop a monitoring and surveillance system to detect diseases, track public health, and to develop a nationwide laboratory network.

Pending Legislation

- H.R. 1132 Critical Infrastructure Earthquake Preparedness Act of 2011 will "direct the Administrator of the Federal Emergency Management Agency to establish a grant program to improve the ability of trauma center hospitals and airports to withstand earthquakes, and for other purposes."[11] This bill is currently in committee.

- There are a number of pieces of pending legislative related to cybersecurity, including the Homeland Security Cyber and Physical Infrastructure Protection Act of 2011, the Cybersecurity and Internet Freedom Act of 2011, and the Cybersecurity and Internet Safety Standards Act.

A number of bills related to general infrastructure development are currently undergoing the legislative process, including, the Sustainable Water Infrastructure Investment Act of 2011.

Conclusion

This is not a comprehensive list of new laws and regulations since September 11, but it does demonstrate the increased focus on securing critical infrastructure and key resources. As America faces challenges from both natural and man-made threats, it is important that we have the appropriate tools in place to effectively mitigate and respond to those challenges. ❖

---

10. http://www.dhs.gov/xabout/laws/gc_1217449547663.shtm.
11. http://www.govtrack.us/congress/bill.xpd?bill=h112-1132.

Transportation *(Cont. from 16)*

constrained within the borders of the United States and thus must deal with the complexity of global regulations and policy. The TSSSP seeks to manage risk in collaboration with industry. Both also seek to grow transportation systems. ❖

Evolution *(Cont. from 6)*

infrastructures as logging requirements are being added and reporting requirements increase. Laws like Sarbanes-Oxley Act and the Gramm-Leech-Bliley Act are reflected globally, and the financial crisis has increased the push toward greater accountability. But in truth, there was little accountability ten years ago and little accountability today. More or less, the lowest level actors involved in any act can be counted on to be punished for top-level acts of malice or incompetence.

Protective Technologies and Approaches:

In essence, there are no widespread new technologies for information protection that have been deployed in the last ten years. Identity management has increased market penetration; data loss prevention methods similar to previous methods for intrusion detection have become more widespread; and trusted platform modules are now widespread. But the overall effect of these changes is apparently negligible and no metrics exist to accurately measure any such effects. Furthermore, the technologies supporting ICS systems have been essentially unchanged over this period, despite dramatic increases in connectivity. This does not bode well for protection of these elements of critical infrastructures. We see more spending on protection in computers, which may reflect increased risk, but again, without metrics...

Conclusions

The one thing we can say with a fairly definitive conclusion with regard to the questions at hand, is that the science and measurement associated with critical infrastructure protection, at least in the information protection arena, has not yet reached the point where even the most basic questions about whether protection is better or worse can be meaningfully evaluated. Without developing a science and system of measurement, we will not be able to answer these sorts of questions ten years from now either. Unfortunately, the main area where we need to make progress in order to make progress in all other areas is an area where we have made no progress.

And time is not on our side. ❖

DHS Evolution *(Cont. from 9)*

instance, on August 3, 2011, DHS published a Notice of Proposed Rulemaking requesting comments on the establishment of an Ammonium Nitrate Security Program. Ammonium nitrate, a chemical commonly used in agriculture and other industries, can also be used by terrorists and other bad actors to make explosives. DHS is proposing an Ammonium Nitrate Security Program through which we would screen prospective buyers and sellers of ammonium nitrate for ties to terrorism. Under the proposed program, we would also work with sellers of ammonium nitrate to verify that prospective buyers have successfully undergone terrorist ties screening before they are able to obtain the chemical. The program also would require those selling ammonium nitrate to retain records and report theft or loss of ammonium nitrate to Federal authorities within 24 hours of discovery.[7]

Protecting Critical Infrastructure is a Shared Responsibility

Homeland security requires active participation at all levels to address constantly evolving threats. DHS continues to work closely with stakeholders to develop solutions for dealing with the uncertainty of risks and to provide our decision-makers with the tools they need to advance critical infrastructure protection. DHS Suspicious Activity Reports, the "If You See Something Say Something™" campaign,[8] retail sector awareness efforts, and bombing prevention training build on shared awareness and responsibility across all levels of government and the private sector. "Our greatest source of strength and our greatest sense of security will always, ultimately, rest not with any machinery, not with any technology, not with any one Federal department, but ... fundamentally on the citizens of our country," Secretary Napolitano recently stated. She added that "...we need, as a country, to keep adapting, to think ahead, to be nimble, and to be adaptive as individuals, as communities, and as a Nation."[9]

In addition to training Federal, State, local officials, and law enforcement, DHS is leading a critical infrastructure higher education initiative designed to ensure that critical infrastructure is included as an essential element of homeland security and other relevant degree and certificate programs. This effort, conducted through George Mason University, is designed to help prepare the critical infrastructure protection workforce of the future by developing and sharing core critical infrastructure protection courses across the academic community. The first year of the program resulted in the development of seven graduate courses in critical infrastructure protection that are currently available to the public through the Center for Infrastructure Protection and Homeland Security Website. The second year of the program, which began in June 2011, will produce a five-course certificate program in critical infrastructure protection as well as an executive master's program with a critical infrastructure protection concentration.

For more information about DHS critical infrastructure protection programs, visit www.dhs.gov/criticalinfrastructure. ❖

7. See DHS Press Release, "Secretary Napolitano Announces Proposed Ammonium Nitrate Program, August 2, 2011, at http://www.dhs.gov/ynews/releases/20110802-napolitano-ammonium-nitrate-security-program.shtm.
8. For more information, see http://www.dhs.gov/files/reportincidents/see-something-say-something.shtm.
9. From the Secretary's speech to the New York University School of Law and the Brennan Center for Justice, June 2, 2011. See http://www.dhs.gov/ynews/speeches/sp_1307479636063.shtm for full transcript of remarks.

Adaptability *(Cont. from 11)*

infrastructure alternatives. Fourth, the financial institutions that provide the resources for security are critical to achieving resilience, and this fourth area is addressed in more detail below in the context of New York area transit.

The City draws upon a number of resources to fund transit recovery and provide security. Transit grant programs from the Federal government include the American Recovery and Reinvestment Act (ARRA) of 2009, the Infrastructure Protection Program's Transit Security Grant Program (TSGP), and the Urban Area Security Initiative (UASI).

From August 13, 2009 through March 15, 2010, New York City obtained almost $1.6 billion in funding under ARRA for transit projects, accounting for 13.9 percent of the total dollar amount awarded nationwide over that period. Other commuter systems that connect to New York City, such as New Jersey Transit, obtained close to a half billion dollars in ARRA funds over the same period, and long distance rail — Amtrak — and the very large number of buses that service the area also obtained funding.[12] The share of funding going to the New York area should be viewed in the context of its share of travel activity and infrastructure.[13] In 2009, New York City's subway system accounted for over two-thirds (68 percent) of the heavy rail passenger ridership. The City of New York is also served by an extensive commuter rail system — the Long Island Railroad and Metro North — which ranked first and third respectively in the number of trips nationwide, each accounting for about a fifth of the trips. In terms of infrastructure, the heavy rail system in New York City accounted for 45 percent of the heavy rail stations and 37 percent of the heave rail track mileage nationwide.

For Fiscal Year (FY) 2010, the New York area received $110,565,000 or 43.7 percent out of a total of $253,000,000 awarded in TSGP grants for bus and rail transit.[14] For FY 2011, MTA, New Jersey Transit, the New York City Department of Transportation, and the Port Authority of New York and New Jersey are four out of a dozen eligible systems categorized as having an Asset on the U.S. Department of Homeland Security Top Transit Asset List (TTAL).[15] These shares are closer to the share of infrastructure the city systems have, and should be sustained over time.

In conclusion, infrastructure systems in and around New York City have demonstrated a considerable amount of innate flexibility and adaptability to the disasters created by the September 11, 2001 attacks. Yet, continuing availability of resources is key to supporting new initiatives to keep the City resilient against the threats of terrorism. It is beyond the scope of this article to present a rigorous evaluation of the extent to which existing funding programs, at least at the Federal level, have supported the City's needs. This would involve a careful matching of needs against funding. However, it is critical that the level of funding not erode and be proportionate to the size of the City's assets and usage, at least as exemplified by the transit funding program. ❖

Rae Zimmerman is Professor of Planning and Public Administration at New York University's Wagner Graduate School of Public Service, where she also directs the Institute for Civil Infrastructure Services. Her areas of expertise are the interconnections among urban infrastructure, environment, security, and extreme events. She is a fellow of the AAAS and fellow and past president of the Society for Risk Analysis.

12. U.S. DOT, FTA, ARRA Grants through 9/30/10. Available at: http://www.fta.dot.gov/news/10536.htm.
13. These percentages are based on annual figures for 2009 calculated from the U.S. Department of Transportation's National Transit Database.
14. U.S. DHS "FY 2010 Preparedness Grant Programs Overview," Transport Security Grant Program (TSGP), (December 11, 2009), available at: http://www.dhs.gov/xlibrary/assets/grants_tsgp_overview_fy2010.pdf.
15. U.S. DHS, op cit., (December 11, 2009), 24.

Restoration *(Cont. from 13)*

public and private.

There was a continual need to coordinate within and among service providers during both the response and recovery phases. Interdependencies among infrastructure systems helped create a need to coordinate the response to disruptive events. Managers of the power infrastructure cannot be expected to know the requirements of, say, a telecommunications provider, and both organizations must be given guidance in order to prioritize their response and restoration activities. Coordination is also required if a firm seeks to reduce its vulnerability, since it may propose a solution that does not consider its interdependencies with other infrastructures.

Finally, there is a need to understand — and continue to consider — the unthinkable. But at the same time we must accept the fact that we are dealing with the future and cannot hope to address all possible contingencies. Personnel in these systems will continue to be called upon to improvise: that is, to bring their experience to bear in a creative and timely fashion. We must therefore plan to improvise, first by understanding the process of improvisation and then developing training to prepare for successful improvisation.

Restoration of critical infrastructure systems following a disaster is normally associated with the so-called restoration phase: that is, the time immediately following disaster response phase, when effort is directed towards saving lives and protecting property from further damage. However, critical infrastructure systems are now recognized as integral to the response phase: firefighting efforts require a stable and ample water supply; rescue vehicles rely on a road network to reach effected persons; and all emergency response personnel require reliable networking capabilities to support communications. ❖

Cybersecurity *(Cont. from 22)*

industry, government, and private citizens. This should also be taken into account in all proposed cyber security legislation.

- Define "cyber" threats in the broadest possible terms, including intentional, unintentional, natural, and other electronic threats, such as Electro Magnetic Pulse (EMP) and electronic warfare against wireless devices. ICS cybersecurity threats are more than botnets and malware.

- Change the culture such that Operations consider security in the same context as performance and safety (not as critical, but important to consider) and IT considers ICS reliability and safety as important as security.

- Establish a means for vetting ICS experts rather than using traditional security clearances or IT certifications.

- Get senior management support as the process fails without it.

If this were a report card, I would give government and industry an E for effort and a D for effective accomplishments. ❖

*A significant portion of this paper was taken from the book, *Protecting Industrial Control Systems from Electronic Threats*, ISBN: 978-1-60650-197-9, May 2010.

Law Enforcement *(Cont. from 19)*

Washington D.C. and the shootings at Virginia Tech on April 16, 2007. Yet, to him, the morning of September 11 still "feels like it was yesterday. You know, ten years later, I think about the event. Are there things I would have done differently? Sure, sure I would have done things differently. I'm sure everybody would have done something different in their life-time. But, I look at it this way: I pray there is never a 9-11 again; I know that's wishful thinking."

The beginning of this article states that it was an honor to interview Virginia State Trooper Michael Middleton. In truth, the word "honor" cannot be stressed enough. Yes, it was his professional obligation to respond to the crash at the Pentagon on that tragic day. However, after speaking with him, it was clear that his actions were the result of something more than duty. Perhaps it is this innate "something" that inspired him and others like him, including Virginia State Trooper Merlin Wimbush and Pentagon Police Officer Donald Behe, to enlist in law enforcement. Regardless of the reason for their service, our Nation perseveres because of their sworn obligation to serve and protect in the face of unknown danger, often at the cost of their own lives.

As the 10th anniversary of this Nation's second day of infamy draws nearer, it is inevitable that the shocking and dramatic footage from that fateful morning will resurface and reawaken old, haunting memories. In the midst of this painful reminiscing, it is important to honor the victims who perished that day, the families they left behind, and the men and women who raced into burning, crumbling buildings while everyone else raced out. Their memory and their bravery are the true backbone of this Nation. ❖

Memorials *(Cont. from 23)*

On September 11, 2008, the Pentagon Memorial was dedicated and opened to the public.[4] The Pentagon Memorial Fund, Inc. was created to fund and preserve the memorial.

The Pentagon Memorial is constructed in the flight path of Flight 77. It contains 184 benches each built over a pool of flowing, lighted water. The flowing water is turned off at 9:37 AM (EST) every morning for a moment of silence for the 184 lost. Each bench has the name engraved of one of the 184 victims. The benches represent the victim's location, whether on-board the plane or in the Pentagon. For the 59 victims on board Flight 77, the benches are arranged so that someone reading the name on the bench will face the sky. For the 125 victims who perished inside the Pentagon, the benches face the south façade of the Pentagon. Additionally, there are "Age Lines"[5] to represent the ages of the victims. The memorial is protected by the United States Pentagon Police.

For more information on the Pentagon Memorial, please visit http://pentagonmemorial.org/.

Flight 93 National Memorial

At 10:03a.m., United Airlines Flight 93 crashed into a field in Shankesville, PA. Forty passengers and crew died heroically as they attempted to thwart the terrorists by gaining control over the hijacked airplane.

On September 24, 2002, President Bush signed into law the Flight 93 National Memorial Act. The Act established a "new national park unit to commemorate the crew and passengers of Flight 93 who, on September 11, 2001, courageously gave their lives thereby thwarting a planned attack on Washington, D.C."[6] Funding provided by a public-private partnership, the Flight 93 National Memorial, is maintained and operated by the National Park Service (NPS). Due to funding constraints and construction plans, the building of the memorial will follow a sequence of phases. The first phase of the memorial will be dedicated during the weekend of the tenth anniversary of September 11. "The Flight 93 National Memorial is the only major September 11 memorial that must still be completed after September of this year," said Neil Mulholland, president and CEO of the National Park Foundation. "…more funding is still needed to properly honor and educate future generations about the actions of the 40 men and women on board Flight 93."[7] The National Park Foundation continues to seek additional funding to complete the remaining elements of the Flight 93 National Memorial.

The plan for the memorial includes a Visitor Center, built in-line with the flight path. The walkway is aligned with 40 Sweet Gum Trees (to commemorate the lives of the 40 passengers and crew of Flight 93) and lead down through the wetlands. The Memorial Plaza will be built along the edge of the crash site, following the fence line established by the County Coroner. On one side of the plaza, there will be 40 white marble walls engraved with the names of the passengers and crew. The memorial is located just outside Shanksville, Pennsylvania and overlooks the "Sacred Ground " (crash-site).[8] Only relatives of the 40 passengers and crew will be allowed to enter the "Sacred Ground."

For more information on the Flight 93 National Memorial, please visit http://www.nps.gov/flni/index.htm. Funding is still needed to complete the memorial; for information on how to support the building of the memorial, please visit http://www.honorflight93.org/join/?fa=ways-to-give. ❖

6. http://www.nps.gov/flni/parkmgmt/upload/PL107226.pdf.
7. http://www.nps.gov/flni/parknews/national-park-service-unveils-new-renderings.htm.
8. http://www.honorflight93.org/news/?fa=viewArticle&articleID=3194.

Changes *(Cont. from 2)*

theory. We are all fond of saying that critical infrastructures are more than the sum of their parts, but it has taken the development of complexity theory to broaden our understanding of how these infrastructures work and why they sometimes break. Viewing critical infrastructures as complex, adaptive systems with emergent properties that make prediction and protection difficult allows us to gain new insights into their strengths and potential fragility.

The third change has to do with mind-set. Resilience has become a watch-word. There are many ways to define "resilience," but the best definition is "the ability to take a punch and get back up again." A decade ago we were focused on protection — building walls — real ones or firewalls — complete with actual or figurative guns, guards, and gates. This attitude has evolved into a more balanced, risk-based approach that puts an ever-increasing emphasis on complementing protection with effective resilience approaches.

As part of the increased emphasis on beefing up resilience capabilities and civil support, DoD has stood up a brigade-sized Consequence Management Response Force (CCMRF) under the day-to-day control of DoD's Northern Command. DoD has also strengthened its liaisons with DHS as well as State and local agencies. All of this is a significant change from the picture in 2001, when DoD had few resources, and little interest, in the areas of homeland defense or resilience.

The fourth change, and one that is still developing, has to do with the realization that critical infrastructures are strategic targets, targets that are particularly vulnerable to cyber-based attacks. Some people deplore this, and worry about the so-called militarization of cyberspace. However, for better or worse, this process is already far down the road and in all likelihood is irreversible.

But that is another story for another time. ❖

Dr. Robert Miller is a Professor at the National Defense University in Washington D.C. In 2001 he was on loan from the Treasury Department as Deputy Director of the U.S. Critical Infrastructure Assurance Office. The opinions expressed here are his own and do not necessarily reflect those of the National Defense University, the Department of Defense, or the U.S. government.

The Center for Infrastructure Protection and Homeland Security (CIP/HS) works in conjunction with James Madison Univerity and seeks to fully integrate the disciplines of law, policy, and technology for enhancing the security of cyber-networks, physical systems, and economic processes supporting the Nation's critical infrastructure. The Center is funded by a grant from the National Institute of Standards and Technology (NIST).

If you would like to be added to the distribution list for *The CIP Report*, please click on this link:
http://listserv.gmu.edu/cgi-bin/wa?SUBED1=cipp-report-l&A=1